ПРИНЯТО
на заседании педагогического совета
протокол № 6 от 5 июня 2015 г.

УТВЕРЖДАЮ
Директор МБУ лицея № 6
_____ Е. Ю.Мицук
приказом № 71 от 5 июня 2015 г.

Положение по защите информации ограниченного доступа в Лицее

Тольятти

1. Общие положения

1.1. Настоящее Положение разработано на основании требований:

Федерального закона Российской Федерации от 27.07.2006 № 152 «О персональных данных»; Федерального закона Российской Федерации от 27.07.2006 149-ФЗ «Об информации, информационных технологиях и о защите информации»; постановления Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»; «Специальных требований и рекомендаций по технической защите конфиденциальной информации», утвержденных приказом Гостехкомиссии России от 30 августа 2002 г. № 282; «Положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного приказом ФСТЭК России от 05.02.2010 №58.

Под информацией ограниченного доступа понимаются сведения, доступ к которым ограничен нормативно-правовыми актами, в частности Указом Президента Российской Федерации от 6.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера».

Персональные данные (далее - ПДн) относятся к информации ограниченного доступа (далее - информация), так как попадают под действие Федерального закона Российской Федерации от 27.07.2006 № 152 «О персональных данных». Цель данного Положения - определение порядка организации, и проведения работ в лицее для построения эффективной системы защиты информации (далее - СЗИ) от несанкционированного доступа, и её последующей эксплуатации. В частности, с целью обеспечение защиты прав и свобод субъектов персональных данных при обработке их ПДн в информационных системах лицея.

1.2. Информационная система (далее - ИС) - совокупность содержащихся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.

1.3. Информационная система персональных данных (далее - ИСПДн) информационная система, представляющая собой совокупность содержащихся в базе данных ПДн, и обеспечивающих их обработку информационных технологий и технических средств.

1.4. Положение предназначено для практического использования должностным лицам ответственным за защиту информации.

1.5. Требования настоящего Положения являются обязательными для исполнения всеми должностными лицами лицея.

1.6. За общее состояние защиты информации в школе отвечает директор лицея.

1.7. Персональная ответственность за организацию и выполнение мероприятий по защите информации в лицее возлагается на сотрудника лицее, назначенного приказом.
1.8. Ответственность за обеспечение защиты информации возлагается непосредственно на пользователя информации в соответствии с инструкцией «По работе пользователей информационной системы», утвержденной директором лицея.
1.9. Проведение работ по защите информации в ИС с помощью встроенных средств безопасности, сертифицированных лицензионных операционных систем и антивирусного программного обеспечения, выполнения требований настоящего Положения, возлагается на ответственного за защиту информации в лицее (далее - ответственный).
1.10. Лица, виновные в нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законодательством.
1.11. При необходимости для оказания услуг в области аттестации ИС можно привлекать специализированные организации, имеющие лицензию на этот вид деятельности.
1.12. Положение может уточняться и корректироваться по мере необходимости.

2.Охраняемые сведения и актуальные угрозы

2.1. Охраняемые сведения - информация, обрабатываемая в ИС лицея в соответствии с «Перечнем сведений конфиденциального характера в лицее», а также представленная в виде носителей на бумажной, магнитной и иной основе.
2.2. Объекты защиты: ИС различного назначения, участвующие в обработке информации, в соответствии с «Перечнем информационных систем»; помещения, где установлены ИС или хранится информация на бумажных носителях.
2.3. Актуальные угрозы безопасности объектов защиты.
В соответствии с моделями угроз безопасности персональных данных в ИСПДн, разработанными и утверждёнными в лицее, актуальными являются только угрозы несанкционированного доступа (далее - НСД) к информационным ресурсам ИС с целью получения, разрушения, искажения и блокирования информации. Применение средств технической разведки для перехвата информации, циркулирующей в ИС лицея маловероятно с учётом её характера. Основное внимание должно быть уделено защите информации, в отношении которой угрозы безопасности реализуются без применения сложных технических средств: обрабатываемой в ИС от НСД нарушителей и непреднамеренных действий сотрудников лицея; выводимой на экраны мониторов

компьютеров; хранящейся на физических носителях; циркулирующей в ЛВС при несанкционированном подключении к данной сети.

3. Организационные и технические мероприятия по защите информации

3.1. Замыслом достижения целей защиты информации от НСД является обеспечение защиты информации путем выполнения требований Положения о методах и способах защиты информации в информационных системах персональных данных, утверждённого приказом ФСТЭК России от 05.02.2010 № 58.

3.2. Целью технической защиты информации в лицее является предотвращение НСД к информации при её обработке в ИС, связанные с действиями нарушителей, включая пользователей ИС, реализующих угрозы непосредственно в ИС, а также нарушителей, не имеющих доступ к ИС, реализующих угрозы из сетей международного информационного обмена с целью её разрушения, искажения, уничтожения, блокировки и несанкционированного копирования.

3.3. Целями организационных мероприятий по защите информации в лицее являются: исключение непреднамеренных действий сотрудников лицея, приводящих к утечке, искажению, разрушению информации, в том числе ошибки эксплуатации АС; сведение к минимуму возможности нарушения политик безопасности с помощью любых средств, не связанных непосредственно с использованием АС (физический вынос информации на электронном носителе).

3.4. Директор лицея самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных п. 1.1. настоящего Положения. К таким мерам могут, в частности, относиться: назначение ответственного за организацию защиты информации; издание комплекта документов, определяющих политику в отношении обработки ПДн в лицее, а также локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации использование для защиты ИС от НСД встроенных средств защиты операционной системы «Windows XP Pro» (и более поздних версий Windows X Pro) установленной на компьютере в соответствии с «Руководством по безопасной настройке»; использование программных (технических средств), сертифицированных по требованиям безопасности информации, для компьютеров с установленной операционной системой отличной от «Windows XP Pro» (и более поздних версий Windows X Pro) или подключенных к сетям связи общего пользования и (или) международного информационного обмена; использование средств антивирусной защиты; предотвращение организационными мерами НСД к обрабатываемой информации;

организация процесса резервного копирования и архивирования как неотъемлемой части политики защиты информации; осуществление учета машинных носителей информации и их хранение в надежно запираемых шкафах; строгое соблюдение сотрудниками лицея «Инструкции по работе пользователей информационной системы».

3.5. Документальное оформление мероприятий по защите объекта информатизации включает: приказ об организации работ по защите информации ограниченного доступа; акты классификации ИС; Положение о порядке организации и проведения работ по защите информации ограниченного доступа в лицее; технические паспорта; приказ о вводе в эксплуатацию; инструкции ответственного и по работе пользователей ИС; журнал учёта паролей пользователей для работы в ИС (при необходимости); журнал учёта машинных носителей информации; «Аттестат соответствия требованиям безопасности» или декларацию о соответствии требованиям безопасности.

4. Ввод в эксплуатацию информационных систем

4.1. Необходимым условием для ввода в эксплуатацию информационных систем лицея является их соответствие требованиям Федерального закона Российской Федерации от 27.07.2006 № 152 «О персональных данных», постановления Правительства Российской Федерации от 17.11.2007 г. № 781 «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и нормативно-методической документации ФСТЭК России по безопасности информации.

4.2. Директор лицея самостоятельно принимает решение по организации работ по построению систем защиты ИС или с привлечением сторонней организации, имеющей лицензию ФСТЭК России на проведения таких работ, или силами самого образовательного учреждения при условии классификации ИСПДн по 3 классу.

4.3. В случае привлечения сторонней организации она проводит аттестационные испытания ИС в соответствии с программой испытаний, согласованной с лицеем. Испытания завершаются выдачей «Аттестата соответствия ИС требованиям безопасности информации».

4.4. В случае проведения работ по построению системы защиты ИС силами самого образовательного учреждения оценка полученного результата проводится в форме декларирования.

4.5. Для декларирования соответствия ИС требованиям п. 3.1 комиссией, утвержденной приказом руководителя ГОУ, подготавливаются и представляются на систему:

акт классификации; технический паспорт; организационно-распорядительная документация разрешительной системы доступа персонала к защищаемым ресурсам;

модель угроз безопасности персональных данных; сертификаты средств защиты информации, используемые при построении системы защиты; инструкция по работе пользователей; инструкция ответственного за защиту информации.

4.6. При использовании для защиты ИС от НСД встроенных средств защиты операционных систем «Windows XP Pro» (и более поздних версий Windows X Pro) их настройка проводится силами самого образовательного учреждения.

4.8. В случае положительных результатов испытаний СЗИ директор лицея декларирует соответствие ИС требованиям безопасности информации.

4.9. По результатам декларирования соответствия ответственным разрабатываются и доводятся до сотрудников школы под роспись «Инструкция по работе пользователей ИСПДн» и рекомендации о порядке выполнения мероприятий по защите информации.

5. Особенности обработки информации, содержащей персональные данные

5.1. Все ПДн субъекта лицея следует получать у него самого (для обучающихся лицея от родителей (законных представителей)). Если ПДн возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо лицея должно сообщить субъекту ПДн о целях, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и последствиях отказа дать письменное согласие на их получение.

5.2. Лицей не имеет права получать и обрабатывать данные субъекта ПДн о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

5.3. Субъект ПДн самостоятельно принимает решение о предоставлении своих ПДн и дает согласие на их обработку.

5.4. Обработка указанных данных возможна без его согласия в соответствии со ст. 6 Федеральным законом от 27.07.2006 № 152 «О персональных данных.

5.5. Согласие на обработку ПДн оформляется в письменном виде.

5.6. Письменное согласие на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта ПДн; цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн; срок, в течение которого действует согласие, а также порядок его отзыва.

5.7. Согласие на обработку ПДн может быть отозвано субъектом ПДн по письменному запросу на имя директора школы.

5.8. Субъекты ПДн не должны отказываться от своих прав на сохранение и защиту тайны

5.9. Субъект ПДн имеет право на получение следующей информации:

сведения о лицах, которые имеют доступ к ПДн или которым может быть предоставлен такой доступ; перечень обрабатываемых ПДн и источник их получения; сроки обработки ПДн, в том числе сроки их хранения; сведения о том, какие юридические последствия для субъекта ПДн может повлечь за собой обработка его ПДн.

5.10. Субъект ПДн вправе требовать от оператора уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

5.11. Сведения о ПДн должны быть предоставлены субъекту ПДн оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам ПДн.

5.12. Доступ к своим ПДн предоставляется субъекту ПДн или его законному представителю оператором при получении письменного запроса субъекта ПДн или его законного представителя. Письменный запрос должен быть адресован на имя директора лицея или уполномоченного руководителем лицо.

5.13. Субъект вправе обжаловать в уполномоченный орган по защите прав субъектов персональных данных (Управление Федеральной службы по надзору в сфере связи и массовых коммуникаций по Москве и Московской области) или в судебном порядке неправомерные действия или бездействия должностных лиц ГОУ при обработке и защите его ПДн.

6. Обязанности и права должностных лиц

6.1. Директор организует работу по построению системы защиты ИС. В частности:

6.1.1. Назначает ответственного за организацию защиты информации из числа сотрудников лицея.

6.1.2. Утверждает состав комиссии по организации работ по защите информации.

6.1.3. Утверждает комплект документов, определяющих политику в отношении обработки ПДн в учреждении, а также локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации.

6.1.4. Утверждает меры и состав средств СЗИ, предложенных для обеспечения безопасности ПДн при их обработке в ИСПДн. При этом оценивает соотношение вреда, который может быть причинен субъектам ПДн и принимаемых мер по защите ИСПДн.

6.2. Заместитель директора по безопасности:

- составляет Перечень сведений конфиденциального характера в школе;
- контролирует работу ответственного по организации и проведению работ по защите информации в лицее;
- предотвращает организационными мерами НСД к обрабатываемой в ИС информации;
- контролирует порядок подготовки, учета и хранения документов конфиденциального характера;
- контролирует порядок передачи информации другим органам и организациям, а также между структурными подразделениями своей организации, лично отвечают за защиту информации, сохранность машинных и иных носителей информации;
- организуют выполнение мероприятий по защите информации при использовании технических средств;
- участвуют в определении мест установки и количества АРМ, необходимых для обработки информации, а также пользователей этих ИС;
- участвуют в определении правил разграничения доступа к информации в ИС, используемых в ГОУ.

6.3. Ответственный:

- разрабатывает организационно-распорядительные документы по вопросам защиты информации при её обработке с помощью ИС;
- контролирует исполнение приказов и распоряжений вышестоящих организаций по вопросам обеспечения безопасности информации;

- знакомит работников школы, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн;
- обеспечивает защиту информации, циркулирующей на объектах информатизации, организовывает работы по декларированию (аттестации) ИС на соответствие нормативным требованиям;
- проводит систематический контроль работы СЗИ, применяемых в ИС, а также за выполнением комплекса организационных мероприятий по обеспечению безопасности информации;
- проводит инструктаж пользователей ИС;
- контролирует выполнение администратором ИС обязанностей по обеспечению функционирования СЗИ (настройка и сопровождение подсистемы управления доступом пользователя к защищаемым информационным ресурсам ИС, антивирусная защита, резервное копирование данных и т.д.)
- контролирует порядок учёта и хранения машинных носителей конфиденциальной информации;
- присутствует (участвует) в работах по внесению изменений в аппаратно-программную конфигурацию ИС;
- определяет порядок и осуществляет контроль ремонта средств вычислительной техники, входящих в состав ИС;
- принимает меры по оперативному изменению паролей при увольнении или перемещении сотрудников, имевших допуск к ИС;
- требует устранения выявленных нарушений и недостатков, давать обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите информации;
- требует от работников представления письменных объяснений по фактам нарушения режима конфиденциальности;
- об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации, а также в случае выявления попыток НСД к информации или попыток хищения, копирования, изменения незамедлительно принимает меры пресечения и докладывает директору лицея; в установленные сроки подготавливает необходимую отчетную документацию о состоянии работ по защите информации.

7. Планирование работ по защите информации

7.1. Планирование работ по защите информации проводится на основании: рекомендаций актов проверок контрольными органами; результатов анализа деятельности в области защиты информации; рекомендаций и указаний Роскомнадзора и ФСТЭК России.

8. Контроль состояния защиты информации

8.1. С целью своевременного выявления и предотвращения НСД к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособность систем информатизации, осуществляется контроль состояния и эффективности СЗИ.

8.2. Контроль заключается в проверке по действующим методикам выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер.

8.3. Повседневный контроль выполнения организационных мероприятий, направленных на обеспечение защиты информации, проводится ответственным.

8.4. Периодический контроль за эффективностью СЗИ осуществляет заместитель директора по безопасности.

8.5. Плановые и внеплановые проверки за соответствием обработки персональных данных требованиям законодательства могут осуществляться территориальными органами Федеральной службы по надзору в сфере связи и массовых коммуникаций.

Допуск представителей этих органов для проведения контроля осуществляется в установленном порядке по предъявлению служебных удостоверений и предписаний на право проверки, подписанных руководителем (заместителем) соответствующего органа.

8.6. Ответственный обязан присутствовать при всех проверках по вопросам защиты информации.

8.7. Результаты проверок отражаются в Актах проверок.

8.8. По результатам проверок контролирующими органами ответственный с привлечением заинтересованных должностных лиц в десятидневный срок разрабатывает план устранения выявленных недостатков.

8.9. Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям и нормам. Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

8.10. При обнаружении нарушений директор лицея принимает необходимые меры по их устранению в сроки, согласованные с органом или должностным лицом, проводившим проверку.